REMARKS / DISCUSSION OF ISSUES

Claims 1-13 are pending in the application.

I. Primary Rejection under 35 U.S.C. §103(a)

The Office has rejected claims 1-3 and 6-13 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003 / 0091186 ("Fontijn") in view of U.S. Patent Publication No. 2002/0141577 ("Ripley"). The Applicants respectfully traverse the rejections.

A. Claims 1-3, 6-7 are allowable

The cited portions of Fontijn and Ripley, individually or in combination, fail to disclose or suggest the specific combination of claim 1.

The Office admits that Fontijn fails to disclose "wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a communication bus." See Office Action, page 3.

The cited portions of Ripley fail to disclose or suggest this feature of claim 1. The Office asserts that the cited portions of Ripley disclose reading a media key block (Figure 3 [block 300]), and the bus key is used to encrypt data transferred from the media or storage reader to the host device or media player (Figure 3 [block 340]). The Office further asserts that Ripley discusses the content scrambling system (CSS) which discloses the use of a single bit called the bus encryption bit to indicate that data is to be encrypted in Sections 4.1 and 4.2. Applicants assert that reference to the CSS for teaching the use of a single bit called a bus encryption bit is improper in light of the intent of MPEP 2124. MPEP 2124 is directed to those circumstances where a factual reference need not antedate the filing date. This section is reproduced as follows:

MPEP 2124

In certain circumstances, references cited to show **a universal fact** need not be available as prior art before applicant's filing date. *In re Wilson*, 311 F.2d 266, 135 USPQ 442 (CCPA 1962). Such facts include the characteristics and properties of a material or a scientific truism. Some specific examples in which later publications showing factual evidence can be cited include

- situations where the facts shown in the reference are evidence "that, as of an application's filing date,
- undue experimentation would have been required, *In re Corneil*, 347 F.2d 563, 568, 145 USPQ 702, 705 (CCPA 1965), or
- that a parameter absent from the claims was or was not critical, *In re Rainer*, 305 F.2d 505, 507 n.3, 134 USPQ 343, 345 n.3 (CCPA 1962), or
- that a statement in the specification was inaccurate, *In re Marzocchi,* 439 F.2d 220, 223 n.4, 169 USPQ 367, 370 n.4 (CCPA 1971), or
- that the invention was inoperative or lacked utility, *In re Langer*, 503 F.2d 1380, 1391, 183 USPQ 288, 297 (CCPA 1974), or
- that a claim was indefinite, *In re Glass*, 492 F.2d 1228,1232 n.6, 181 USPQ 31, 34 n.6 (CCPA 1974), or
- that characteristics of prior art products were known, *In re Wilson*, 311 F.2d 266, 135 USPQ 442 (CCPA 1962)." *In re Koller,* 613 F.2d 819, 823 n.5, 204 USPQ 702, 706 n.5 (CCPA 1980) (quoting *In re Hogan,* 559 F.2d 595, 605 n.17, 194 USPQ 527, 537 n.17 (CCPA 1977) (emphasis in original)).

However, it is impermissible to use a later factual reference to determine whether the application is enabled or described as required under **35 U.S.C. 112**, first paragraph. *In re Koller*, 613 F.2d 819, 823 n. 5, 204 USPQ 702, 706 n.5 (CCPA 1980). References which do not qualify as prior art because they postdate the claimed invention may be relied upon to show the level of ordinary skill in the art at or around the time the invention was made. *Ex parte Erlich*, 22 USPQ 1463 (Bd. Pat. App. & Inter. 1992).

Applicants respectfully submit that the Office has improperly used the MPEP 2124 exception, by citing the AACS as a later factual reference in an attempt to show that the AACS Specification recitation of: "a single bit called the bus encryption bit to indicate that data is to be encrypted in Sections 4.1 and 4.2" is a universal fact. Applicants respectfully submit that the teachings of the AACS Specification do not constitute a "universal fact". A universal fact, as defined by MPEP 2124, include the characteristics and properties of a material or a scientific truism. The **Advanced Access Content System (AACS)** is an ISO format standard for the distribution and protection of media content. It's main intent is to restrict access to and copying of DVD-optical-discs. A "fair-play" digital rights system for the next generation. It is well known that in the arena of media and media content multiple standards survive and thrive. A system can choose to conform or not to distribute and protect its media content. Further, Ripley explicitly discloses a method for utilizing a bus key and an MKB, neither of which are sector oriented. That is, Ripley describes a viable system that is non-compliant with the ISO standard. Applicants submit that the AACS standard does not meet the threshold of a so-called "universal fact" within the definition of MPEP 2124. Accordingly, it is respectfully submitted that MPEP 2124 is an improper reference.

In addition, Applicants further assert that the cited portions of Ripley fail to disclose or suggest this element of claim 1 for at least the following reasons. The objectives of Ripley are different from that of the present invention and consequently the methods and systems employed by each are in stark contrast. Specifically, the invention is directed to the idea of signaling a read-out device that **particular user data** shall be encrypted by the read-out device before the particular user data is transmitted over a communication bus. Thus, encryption indication information is provided in the management information **and associated with all sectors in which user data are stored** which is encrypted before transmission over the communication bus. This encryption indication information will be read and evaluated by the read-out device which then encrypts the associated user data before they are outputted to the communication bus.

Ripley is directed to a renewable protection system which utilize an MKB 210 as a block of encrypted data that allows different devices using different individually-assigned device keys to extract a common secret key, called the media key. If a set of device keys is compromised at some future point, a new MKB can be used to exclude just the set of compromised device keys from the system. As part of the copy protection system 200 of Ripley, new compliant DVD drives 202 are equipped with device keys 218, MKB processing logic 220, one-way function 224 and encryption logic 228 necessary to process the MKB and extract its secret media key 222, to calculate a bus key 226 based on the media key 222 and a nonce 250, and encrypt the data 212 on the DVD 208, which is CSS scrambled, using the bus key 226. *See* Ripley, pars. 23 and 24.

It is submitted that there is no teaching or suggestion in Ripley that either the bus key or the MKB is sector oriented. Rather, the bus key encrypts all of the data with no distinction to which sector is being referenced. With regard to the MKB, as is well known in the art, an MKB typically has a size that may range from at least a few kilobytes to up to a few hundred kilobytes, depending upon the number of device keys that have been revoked. If an MKB of this size were to be utilized on a sector by sector basis, this would be wasteful of the available space on a storage medium. In other words, it would be wasteful to employ a different and potentially very large MKB for each individual sector on the storage medium (e.g., a typical sector size on a DVD or Blu-Ray Disc is 2-kilobytes, which implies an overhead of 3200%, in case that the management information (M) would consist of a 64-kilobyte MKB). In addition, there is the issue of the additional overhead of the protocol in which the host would have to generate and communicate once for each MKB on the storage medium in order to transform the media key contained in the MKB to a bus key.

Thus, the cited portions of Fontijn and Ripley, individually or in combination, do not disclose or suggest "*wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a*

communication bus", as recited in claim 1 (Emphasis Added). Hence, claim 1 is allowable.

Claims 2-3 and 6-7 depend from claim 1, which Applicants have shown to be allowable. Thus, claims 2-3 and 6-7 are allowable, at least by virtue of their dependency from claim 1.

B. Claims 8-13 are allowable

Independent Claims 8-11 and 13 recite similar subject matter as Independent Claim 1 and therefore contain the limitations of Claim 1. Hence, for at least the same reasons given for Claim 1, Claims 8-11 and 13 are believed to be allowable over the cited references in any reasonable combination.

Claim 12 depends from claim 11, which Applicants have shown to be allowable. Thus, claim 12 is allowable, at least by virtue of its dependency from claim 11

II. Further Claim Rejections under 35 USC 103

The Office has rejected claim 4 under 35 U.S.C. §103(a), as being unpatentable over Fontijn in view of Ripley and in further view of U.S. Patent No. 6,378,072 ("Collins"). Applicant respectfully traverses the rejection.

A. Claim 4 is Allowable

As explained above, the cited portions of Fontijn and Ripley do not disclose or suggest each and every element of claim 1, from which claim 4 depends. Specifically, the cited portions of Fontijn and Ripley fail to disclose or suggest "*wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a communication bus" (Emphasis Added).* Collins does not disclose the elements of claim 1 that are not disclosed by Fontijn and Ripley. Collins is

merely cited by the Office for remedying a deficiency in Fontijn and Ripley. Specifically, Collins is cited for teaching a plurality of encryption algorithms to secure a communications bus. *See* Collins, col. 6, lines 5-27. Hence, there is no teaching or suggestion in Collins of "*wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a communication bus",* as recited in claim 1. Therefore, the combination of Fontijn, Ripley and Collins do not disclose each and every element of claim 1, from which claim 4 depends. Hence, claim 4 is allowable.

C. Claim 5 is Allowable

As explained above, the cited portions of Fontijn and Ripley do not disclose or suggest each and every element of claim 1, from which claim 5 depends. Specifically, the cited portions of Fontijn and Ripley fail to disclose or suggest "*wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a communication bus" (Emphasis Added).* Taki does not disclose the elements of claim 1 that are not disclosed by Fontijn and Ripley. Collins is merely cited by the Office for remedying a deficiency in Fontijn and Ripley. Specifically, Taki is cited for teaching a key-heirarchy information for determining which key-heirarchy is to be used for determination of a content key. *See* Taki, Figs. 4, 8 and 23 and par. 0001.

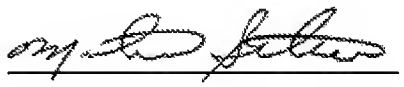
Hence, there is no teaching or suggestion in Taki of "*wherein said management information (M) comprises an encryption indication information (M1) comprising a single bit associated with each of said sectors (S), each bit indicating to a read-out device whether the user data stored in the associated sector (S) are to be encrypted by the read-out device (2) before being transmitted over a communication bus",* as recited in claim 1. Therefore, the combination of Fontijn, Ripley and Taki do not disclose each and every element of claim 1, from which claim 4 depends. Hence, claim 5 is allowable.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1-13 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Mike Belk, Esq., Intellectual Property Counsel, Philips Electronics North America, at 914-945-6000.

Respectfully submitted,



Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001